Secur J (2018) 31:410–427
https://doi.org/10.1057/s41284-017-0107-0

ORIGINAL ARTICLE

Private intelligence in the Republic of Slovenia: theoretical, legal, and practical aspects

Jaroš Britovšek[1] · Bojan Tičar[2] · Andrej Sotlar[2]

Published online: 23 June 2017

Abstract The article explores elements of private intelligence in the Republic of Slovenia (hereinafter Slovenia) using a combination of theoretical, legal, and practical aspects. The theoretical aspects define and explain intelligence through its fundamental elements and concepts. These fundamental elements are then further utilized in the context of legal aspects to identify the main private intelligence actors in Slovenia. Finally, the practical aspects of private intelligence were researched with an online survey among companies dealing with private detective investigations, private security, information security, and security consulting. The exact spread and impact of private intelligence and counterintelligence in Slovenia is definitively not easy to assess. However, an analysis of legal framework and findings from online survey suggest that there are identifiable but limited elements of private intelligence and counterintelligence, with the latter primarily limited to passive protective measures, mostly performed by private detectives and private security companies. Although it is likely difficult, further research of corporate use of intelligence and counterintelligence in Slovenia would be needed.

Keywords Intelligence · Private intelligence · Private counterintelligence · Private detectives · Private security

✉ Andrej Sotlar
andrej.sotlar@fvv.uni-mb.si

Jaroš Britovšek
jaros.britovsek@mors.si

Bojan Tičar
bojan.ticar@fvv.uni-mb.si

[1] Ministry of Defense of the Republic of Slovenia, Vojkova cesta 55, 1000 Ljubljana, Slovenia

[2] Faculty of Criminal Justice and Security, University of Maribor, Kotnikova ulica 8, 1000 Ljubljana, Slovenia

Introduction

Intelligence has long been perceived as a classical example of a state function, but in recent decades, it made its way into the private sector as well. However, the privatization of intelligence or the implementation of intelligence elements in the private sector has primarily been observed in the West and in the USA in particular (Gill and Hart 1999; Hulnick 2002; Chesterman 2008; Keefe 2010; Javers 2011). Trend of private security industry growth has been observed also in the European Union (EU; van Steden and Sarre 2007), so questions arise if similar developments are also taking place in the Republic of Slovenia (hereinafter Slovenia). The country of our research focus is therefore Slovenia, a relatively small country with population of just over 2 million, now a member of the EU, which witnessed the transformation from socialism to democracy and towards free market capitalism in 1990. Since then, Slovenia has often copied the ideas and trends coming from Western countries. Therefore, we attempted to find out if the same process or elements of private intelligence as in the West can also be found in Slovenia. To find out, we focused our research efforts on the legal and practical aspects of private detective and security personnel in Slovenia. That is, have private actors in Slovenia taken on the once state-dominated functions of intelligence? In an effort to answer these questions, this article aims to examine private intelligence in the Republic of Slovenia through theoretical, legal, and practical aspects.

Based on a literature review and historical examination of the evolution of intelligence as a state function, we were able to derive a theoretical and conceptual framework to define and analyze intelligence, including private intelligence. Intelligence itself is a broad concept, but at its core it is concerned with data and information, and consists of the following three fundamental elements: (1) data collection, (2) analysis, and (3) counterintelligence. The latter being an important element of data protection. In addition to the above core elements, other concepts that define and distinguish intelligence from other forms[1] of data collection include risk, secrecy, and surveillance (Britovšek and Sotlar 2014). The theoretical model developed and used in this article supported the systematic review of intelligence-related legislation, as well as the conduct of an online survey of businesses involved in private security, security advising, information security, and private detective services. At first, we tried to find respondents in private (security) business to conduct in-depth interviews on the topic of private intelligence in Slovenia. However, the responses were limited and most were reluctant to talk about this topic, likely due to the negative connotation the word "intelligence" is perceived in post-socialist countries (Williams and Deletant 2001). From limited conversation with them, we found out that many of them equate the term "intelligence" with "spying." We therefore decided to create an online survey asking respondents how often they conduct listed activities that are considered (at least in theory) to be part of intelligence or counterintelligence activities.

[1] Other forms of collection can be for example data collection for academic purposes or general data collection for customer services. The paper is more focused on the gathering data on threats, meaning the defensive nature of intelligence.

Some political and economic features of Slovenia

Slovenia is a small transition economy, geographically located between Western Europe and the Western Balkans, and highly dependent on foreign trade (mainly with Germany, Italy, Austria, and Croatia). The country transitioned to democracy and relatively successful market economy with current GDP per capita around 32.000 USD. Slovenia is a member of Organization for Economic Co-operation and Development, Organization of Security and Cooperation in Europe, Council of Europe, and many others, while the most important memberships are those in United Nations, EU, and North Atlantic Treaty Organization (NATO).[2] By adopting Euro as its currency, Slovenia became a member of Economic and Monetary Union in 2007 (Central Intelligence Agency 2017). The country used gradualism instead of swift reforms to transform its economy and the strategy seemed to be working, as the initial high growth rates managed the country to reach the EU average per capita income relatively rapidly. However, the protracted gradualism likely led to increase of political interference in managing of state-owned companies and banks, and rise of managing elite, which defended national interests in those companies. The privatization of state-owned companies and banks has effectively been stopped or at least slowed down (Guardiancich 2016). The state is still relatively heavily involved in the economy, which can lead to privileged position of state-owned companied, and can consequently make it harder for private entrepreneurial initiative to flourish.

The research of private intelligence in Slovenia is limited. Vršec (1993) was one of the first to recognize the importance of data collection in the private sector, although when referring to the collection and data analyzing in the private sector he tried to avoid using the term "intelligence." He used the term "economic enquiries" (svn. gospodarsko poizvedovanje), which has since been adopted and used by other Slovenian authors (such as, Dvoršak 2003; Gjerek 2009; Žaže 2007). On the other hand, Vrenko (1999), when surveying market research, adopted an English speaking term "competitive intelligence" (svn. konkurenčna obveščevalna dejavnost). Podbregar (2005, 2006) wrote about the negative aspects of intelligence in the private sector, particularly focusing on "industrial espionage." The paper aims to build on these foundations and upgrade the knowledge on utilization of intelligence-related tasks in Slovenia's private sector.

Theoretical aspects of intelligence

The authors' aim is to establish a theoretical and conceptual framework of intelligence. The theoretical aspects have to be useful in defining and identifying intelligence in different areas, including the private sector, and also as a tool to distinguish intelligence from other forms of data collection. In order to conduct a study on private intelligence, we had to derive a suitable and workable definition and theory for intelligence generally. Through the literature review, several definitions of intelligence and a historical evolution of intelligence were examined,

[2] Slovenia joined EU and NATO in 2004.

allowing us to identify foundational elements and premises that constitute a viable and workable definition of intelligence. First of all, intelligence works in an environment of data and information. Thus, when writing about intelligence, it is important to consider concepts that distinguish intelligence collection from other forms of data collection. We identified these distinguishing concepts as risks, surveillance, and secrecy.

The concepts were not chosen at random, but through a careful literature review of the theory and definitions of intelligence. Matey (2005) said that intelligence must be able to warn decision-makers of upcoming crises and must foresee or detect threats that they might face. Thus, the first identified concept of intelligence is *risk*. Risk, as a defining concept of intelligence, was identified by Warner (2009), who saw intelligence as a service for or interaction with leaders to manage risks that are derived from competition with adversaries and foes. Similarly, Wheaton and Beerbower (2006) saw intelligence as a tool for decreasing risks and acquiring a competitive edge for decision-makers vis-à-vis their competitors. Intelligence therefore deals with, manages, and aims to limit the risks that decision-makers or leaders face.

The second foundational concept is *surveillance*, which Gill and Phythian (2006) identified as one of the most fundamental concepts of intelligence. According to them, surveillance is defined through two elements: collection/storing of data and information, and control over human behavior; or, in other words, information and power. They see intelligence as a subsystem of surveillance. Intelligence is concerned with data collection and analysis, and also the application of finished intelligence reports that can be used to practice power and influence people or organizations towards ones will. One should understand that intelligence is part of a broader political or economic tool, the aim of which is to take measures to limit risks based on intelligence reporting.

The third concept identified is *secrecy*. Shulsky and Schmitt (2002) see intelligence as a kind of silent warfare, where opponents try to neutralize each other's intelligence efforts. One side's intelligence failure is the other's counter-intelligence success. Therefore, secrecy (that is, protecting one's own sensitive information and activities) is seen as one of the most important concepts of intelligence (Gill and Phythian 2006; Warner 2009). Secrecy is perceived as a normal concept in every organization, especially in a highly competitive environment. Its implication can often be recognized in the practice of the "need to know" principle (Colby 1976). Intelligence exists because decision-makers try to hide their information from competitors, consequently leading competitive decision-makers to strive for that information (Lowenthal 2009).

In the intersection of concepts such as risks, surveillance and secrecy lay the core of intelligence. Apart from the mentioned concepts, intelligence can be explained through its fundamental elements: data collection, intelligence analysis, and counterintelligence (Fig. 1).

The first fundamental element of intelligence—*data collection*—can be categorized according to different intelligence disciplines. Among these, the most important are the following:

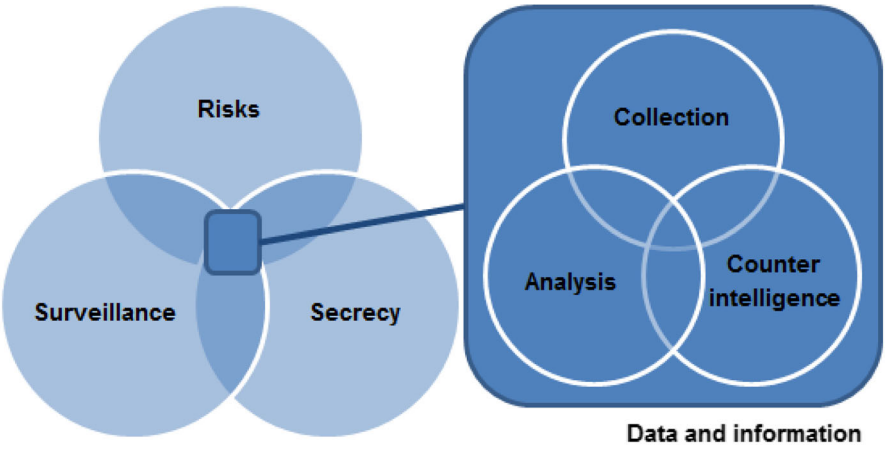

Fig. 1 Fundamental concepts and elements of intelligence

- Open source intelligence, meaning the collection of data from publically available sources (the news media, databases, publications, etc.);
- Human intelligence, meaning the collection of data through people (spies, agents, insiders, informants, diplomats, businesspersons, tourists, etc.);
- Signals intelligence, meaning the intercepting and collecting of data over electronic means of communications (radio, radar, networks, etc.);
- Imagery intelligence, meaning the collection of imagery data from different perspectives (photography, video, infrared technology, etc.) (Wyss 2011).

The collected data and information must later be analyzed, meaning that they have to be collated, compared and assessed. Lowenthal (2011) saw *analysis* as one of the most important elements of intelligence, as the end product of analysis is an assessment, which is crucial in supporting the decision-makers by providing context and supporting evidence. Other elements of intelligence are seen as a support to intelligence analysis, providing and collecting the needed data and information. Analysis also deals with data and information collected and provided by the third element of intelligence, namely counterintelligence.

Counterintelligence is seen as a complementary part of intelligence and can additionally be divided into two parts: passive and active (Whitehead 2003; Prunckun 2012). The aim of both active and passive counterintelligence is to protect sensitive information and neutralize intelligence threats (such as espionage, sabotage, subversion, and terrorism). The line between them is often blurry, as they can intertwine. Passive counterintelligence basically encompasses protective measures, such as physical, technical, or organizational. Active counterintelligence refers to more dynamic activities, such as counterintelligence investigations, data collection on intelligence threats and thwarting opposing sides' intelligence efforts (Prunckun 2012).

Evolution of private intelligence

Intelligence activity is as old as humanity itself and has since then been a subject to modernization, professionalization, and specialization. The main function of intelligence has always been to support the ruler. As an activity, it has been often equated with simple spying. However, modern intelligence has evolved through different forms of organization, beginning with military intelligence, security intelligence, and national intelligence, and later diversifying into more specialized forms of organization, newly established according to intelligence discipline or method of collection (Herman 1996). At the same time, and with the advent of the private economy, intelligence also made its way into the private sector.

Alongside military power as a prevailing method of political domination, the rise of economic power encouraged rulers to shift their focus increasingly to their economies to enhance political domination. Rulers started establishing companies and gathered information on the economic power and industrial capacities and secrets of competitor states. With the rise of industry, private sector or private companies became increasingly more important players. The growth and spread of private sector and private companies also encouraged the establishment of first forms of private intelligence. These companies mainly had their roots in the USA and were first formed as private security or private investigative (that is, private detective) companies (Weiss 2008).

Today, primarily in the Western world, we find several private companies that offer intelligence or counterintelligence services in the marketplace (Bean 2015). This situation and the process of establishing such private companies accelerated by the end of twentieth century, with three main factors contributing to this process: (1) the end of the Cold War, (2) the liberalization of security-related services, and (3) the spread of information and surveillance technology. The end of the Cold War ended the bitter rivalry between two antagonistic blocs, both of which had substantial intelligence and security apparatuses. Many intelligence and security personnel started moving into the private sector and brought with them their skills and knowledge (Blancke 2011; Campbell 2013a). The liberalization of security-related services enabled the employment of these professionals and also brought new services to the market typical of intelligence and counterintelligence (Chesterman 2008; Keefe 2010). The advancement of information and surveillance technology, especially the internet, enabled rapid access to information and provided tools to a wider population, bringing to an end the relative monopolization of information by state intelligence services (Dedijer 2003; Campbell 2013b).

As already mentioned, private intelligence companies in the West started to appear after the Second World War, but their numbers rapidly increased after the end of the Cold War. However, the origins of private intelligence can be found in nineteenth century USA. In this period, the first private detective and security companies were established, which later led to private intelligence and counter-intelligence companies (Weiss 2008). To research the assumption that similar processes are going on in Slovenia we will combine intelligence theoretical aspects

with legal and practical aspects of private detectives and the private security industry (including security consulting and information security) in Slovenia.

Legal aspects of private intelligence in Slovenia

Using the theoretical aspects of intelligence and its fundamental elements, we were able to identify relevant legal documents in Slovenia that could enable or at least permit private intelligence activities to take place. Some elements of private intelligence were found in the Private Detective Activities Act (2011) and the Private Security Act (2011). Because intelligence activity carries with it the inclination to infringe upon certain human rights, especially the right for privacy, Slovenia established protective legal mechanisms through the Constitution of the Republic of Slovenia (1991) and the Personal Data Protection Act (2004). Any unauthorized and unlawful interventions or breaches of human rights are punishable under the Criminal Code of the Republic of Slovenia (2008).

The collection and analysis of data in the private sector are limited for private citizens mainly to open source collection. However, private detectives and partially private security personnel have certain legal entitlements that enable them to collect data and information beyond what is permitted for ordinary citizens. According to the Private Detective Activities Act (2011), private detectives operate under certain legal conditions that enable them to gather data and information on behalf of their clients. A private detective is entitled to (1) collect data directly from persons or publicly accessible sources, (2) acquire data from government records (vehicle registration…), (3) engage in surveillance, (4) and utilize some limited technical means of collection, such as image and sound recording. In the theoretical aspects of intelligence, we also mentioned analysis, which is simply the cognitive process of manipulating and working with data and information, rendering a legal framework of analysis obsolete and unnecessary. Meaning that, if one has already been permitted to collect information, no further legal authorization to analyze that information is needed.

As already mentioned, counterintelligence can be divided into active and passive forms. Counterintelligence in the private sector is mainly conducted by passive measures, meaning the denial and protection of sensitive information from unauthorized individuals or organizations. The manifestation of private counterintelligence elements can be seen in the implication of the protection of secrets in the private sector. Such protection of industrial, commercial, and trade secrets in Slovenia is guaranteed by the Employment Relationship Act (2013), Code of Obligations (2001) and Companies Act (2006). The Criminal Code of the Republic of Slovenia (2008) also prohibits and sanctions unlawful disclosure of professional secrecy,[3] violation of secrecy of means of communication (e.g., unauthorized opening of private letters) or unauthorized access into business information systems.

[3] Criminal Code of the Republic of Slovenia (2008) defines it as unlawful discloser of a secret which a person got access to due to their professional position as a counsel for the defence, lawyer, doctor, priest, social worker or psychologist or by way of performing any other profession.

Indeed, the importance of and need for the protection of trade secrets have been acknowledged by the EU as well, of which Slovenia is a member. In 2016, the Council of the EU adopted a new directive setting out rules for the protection of trade secrets and confidential information of EU companies (Council of the EU 2016).

The legislation in Slovenia enables counterintelligence mainly in its passive protective measures (physical, technical, and organizational security or protective measures) and partly more active counterintelligence such as investigations. The Private Detective Activities Act (2011) lists the areas of work for private detectives in Slovenia. Private detectives are allowed to conduct the collection of data and information as it relates to adherence to non-competition clauses and agreements. Private detectives can therefore deter, prevent, and investigate the leaking of data and information to their clients' competitors. They are able to collect information about criminal offences and the perpetrators of such criminal offence regarding actions such as disclosure and unauthorized acquisition of trade and professional secrets. Additionally, private detectives can perform certain elements of counter-intelligence by consulting to their clients regarding the prevention of theft or leaking of secrets. Lastly, private detectives can plan and implement measures to protect trade and professional secrets, information systems, economic, and personal data and information.

The Private Security Act (2011) allows private security personnel to also carry out certain passive counterintelligence measures in Slovenia. The Private Security Act (2011) encompasses several types of private security licenses. According to the theoretical aspects of intelligence, physical counterintelligence measures can be identified in the following security licenses: protection of property, protection of persons, and the transportation and protection of currency and other valuables. Additionally, technical counterintelligence measures can be identified in the following security licenses: the operation of a security control center,[4] the design of technical security systems and the implementation of such systems.

Due to the increased development and dependency on information and communication technology, today's sensitive information is largely stored or transferred in communication databases and networks. The Electronic Communications Act (2012) regulates the protection of such networks in Slovenia. The act defines the duties and responsibilities of private operators that deal with communication networks. It also demands that operators prepare a security plan in case of incidents and emergencies.

As mentioned before, the aim of intelligence is to collect relevant information, which carries with it a risk of jeopardizing one's right to privacy. Alongside its own legislation, Slovenia is also bound by international legal agreements that protect basic human rights and freedoms, including the right to privacy, which is most

[4] Security control center is basically a unit or room from which operators can monitor security issues on an organizational and technical level. According to the Private Security Act (2011), operation of a security control center means the management and constant physical control by SCC operators of installed technical security systems, systems and devices for protection of persons, property, an area or a protected person, as well as control of telecommunication paths for the transmission of alarm signals, performed in the SCC.

relevant to this article. Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966/1976) both state that no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence. Additionally, The European Convention on Human Rights (1953/2010) protects the right to privacy in one's personal and family life, home, and correspondence. The right to privacy is also protected by Article 35 of the Constitution of the Republic of Slovenia (1991). While the Personal Data Protection Act (2004) further regulates the handling and protection of personal data in more detail, the Criminal Code of the Republic of Slovenia (2008) explicitly forbids any activities that would jeopardize one's right to privacy. These protective measures safeguard one's right to privacy and create legal limits to private intelligence in Slovenia.

We identified private detectives and private security personnel (including security advisers and information security professionals) as leading contenders for intelligence in Slovenia's private sector. As Sotlar and Trivunovic (2012) explained, private detective powers regarding the collection of information are always accompanied by fears or risks of private detectives gaining powers similar to those usually associated with the state's security and intelligence services. Therefore, private detectives and private security personnel who hold licenses are, according to the Private Detective Activities Act (2011) and the Private Security Act (2011), forbidden from carrying out tasks that are legally reserved for the police, the Slovenian Intelligence and Security Agency (SOVA) and the Intelligence Security Service (OVS). Private detectives are also not allowed to engage in private detective services on behalf of domestic or foreign security or intelligence agencies, political parties or organizations that were established by political parties. This however does not exclude intelligence being conducted in the private sector, as it only limits consumers of private intelligence to the private sector.

Interfering with one's rights is also limited in one's place of work. That is, the right to privacy extends to the workplace. The European Court of Human Rights, which is responsible for all matters regarding the interpretation and implementation of the European Convention on Human Rights (1953/2010), decided in the case Halford versus the United Kingdom ([1997] ECHR 20605/92) that the right to privacy can apply to workplaces, depending on whether there is a reasonable expectation of privacy. The court decided similarly in the case Copland versus the United Kingdom ([2007] ECHR 62617/00), where it emphasized an expectation of privacy when an employee was given prior warning that workplace communications systems were liable to monitoring. However, in the case Barbulescu versus Romania ([2016] ECHR 61496/08) the court decided in favor of the employer, as the employer did have an absolute ban on employee's use of work equipment for private purposes and the surveillance of the employees' communication had basis in the ban. Klemenčič (2001) states that there is a collision of three interests when implementing security in private companies: the interests of the employer, the interests of the employee, and third party interests. The employer expects that his equipment will be used in accordance with the companies' goals. The employee, on the other hand, expects a certain level of privacy at work, especially if there are no

warnings about possible surveillance. Lastly, a third party can unknowingly fall under surveillance if he communicates with the employees.

All the above-mentioned legal documents allow the existence, albeit limited in nature, of private intelligence in Slovenia. Besides the collection of data and information through openly accessed sources, which is not restricted to the wider public, we can conclude that private detectives in Slovenia are allowed or enabled to acquire data from government records, engage in surveillance, and utilize image and sound recording. Analysis, as a cognitive process and methodology, can be implemented regardless of legal framework. Additionally, legislation in Slovenia also partially enables the use of private counterintelligence, although limited to more passive security or protective measures, such as physical and technical security.

In the next section, we present the practical aspects of private intelligence in Slovenia on the basis of the opinions of private detectives and private security personnel (including private security advisers and information security professionals) on this subject.

Practical aspects of private intelligence in Slovenia

Theoretical and legal aspects of private intelligence in Slovenia enabled us to select a group that would be suitable for additional research. Due to the reasons explained in introduction section of the article, in order to research the practical aspects of private intelligence in Slovenia, we decided to use an online survey specifically targeting businesses involved in private security, information security, security consulting, and private detective services. These businesses were selected because private security practitioners (including security advisers) and private detectives were the pioneers of private intelligence in the USA. We decided to add information security professionals as the modern security relies heavily on information technology. The online survey was constructed with the online research tool 1KA. The tool 1KA is an open code application that supports online surveys. It has three main components: (1) support for research, construction, and management of online questionnaires, (2) execution of the online survey (that is, the invitation to potential correspondents and collection of data), and (3) statistical analysis of the collected data (1KA 2016).

We wanted to find out if any of the elements of intelligence discussed in the theoretical and legal aspects can be found amongst private sector practitioners in Slovenia. The questions in the survey were divided into two parts: quantitative and qualitative. In the first part, we asked respondents to name their main activity (private security, private detective, information security, and security consulting). We continued with questions on how often they conduct certain activities that we identified as part of private intelligence or counterintelligence. We also asked them how often they collect information for their customers on different topics (foreign market situation, domestic market situation, their employees, their business partners, and their competition). Then we wanted to know how often they used particular methods in collecting information. Additionally, we wanted to know how

often they witnessed different intelligence threats during their work (espionage, sabotage, subversion, and terrorism). In the final part of quantitative questioning, we wanted to know if they perceive some of their work as private intelligence or counterintelligence. According to the last question, we divided the respondents into two groups: Group 1, encompassing respondents who perceived their work as intelligence or counterintelligence, and Group 2, encompassing respondents who answered that they do not perceive their work as intelligence or counterintelligence.

The second part of the questionnaire was qualitative. Here, we tried to solicit explanatory answers regarding respondents' opinions on private intelligence and counterintelligence in Slovenia. Although we defined counterintelligence as an essential part of intelligence, we separated the two concepts when asking the respondents their opinions on each. We tried to avoid any confusion among respondents and also sought to keep respondents from focusing only on information collection, with which intelligence is often conflated.

The online survey was sent to 209 online addresses of private companies and individuals who are involved in private security, private detective work, information security, and security consulting. The online addresses were found in the databases of private security licenses and private detectives, and through online searches for private companies involved in security consulting and information security. The final sample was random. The survey started on the 16th of September 2013 and was completed on the 16th of December 2013. Out of 209 selected addresses, 134 respondents clicked on the first page, 72 engaged the survey, but only 59 respondents completed the survey, constituting 40% of those contacted.

Among those who completed the survey, 21 (36%) respondents perceived some of their work as private intelligence or counterintelligence, and 38 (64%) respondents did not see any resemblance between their work and private intelligence or counterintelligence. As mentioned above, the former encompass Group 1 and the latter encompass Group 2 (Chart 1). Private detectives and private security personnel dominate both groups. In Group 1; 11 (52%) respondents were working as private detectives, 5 (24%) in private security, 4 (19%) in security consulting, and one (5%) in information security. In Group 2; 19 (50%) respondents

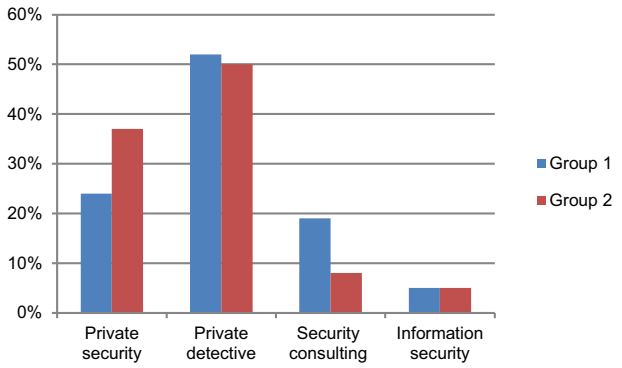

Chart 1 Respondents' field of work: *Group 1* ($n = 21$) and *Group 2* ($n = 38$)

were working as private detectives, 14 (37%) in private security, 3 (8%) in security consulting, and 2 (5%) in information security.

It has to be noted that respondents could have interpreted the terms we offered them to choose from in the questionnaire very subjectively, which highlights the issue of connotation or understanding of intelligence and terms related to it. The activities and terms were chosen through intelligence literature review and consultation with limited number of experts. Some of the activities could also overlap, such as observation and surveillance or technical security and bug sweeping, which could be part of technical security, although not necessarily. Also, as we did not follow up on some answers, such as terrorism, and can therefore not be sure what they meant precisely by that term. The list is not perfect, but it gives us enough indications of certain activities being conducted or noticed by the respondents.

We found out that respondents who perceived some of their work as related to intelligence and counterintelligence also more often performed tasks that we identified as private intelligence and counterintelligence. Comparing Groups 1 and 2 regarding the question of how often they conduct certain activities associated with private intelligence and counterintelligence (Chart 2), we found that Group 1 has,

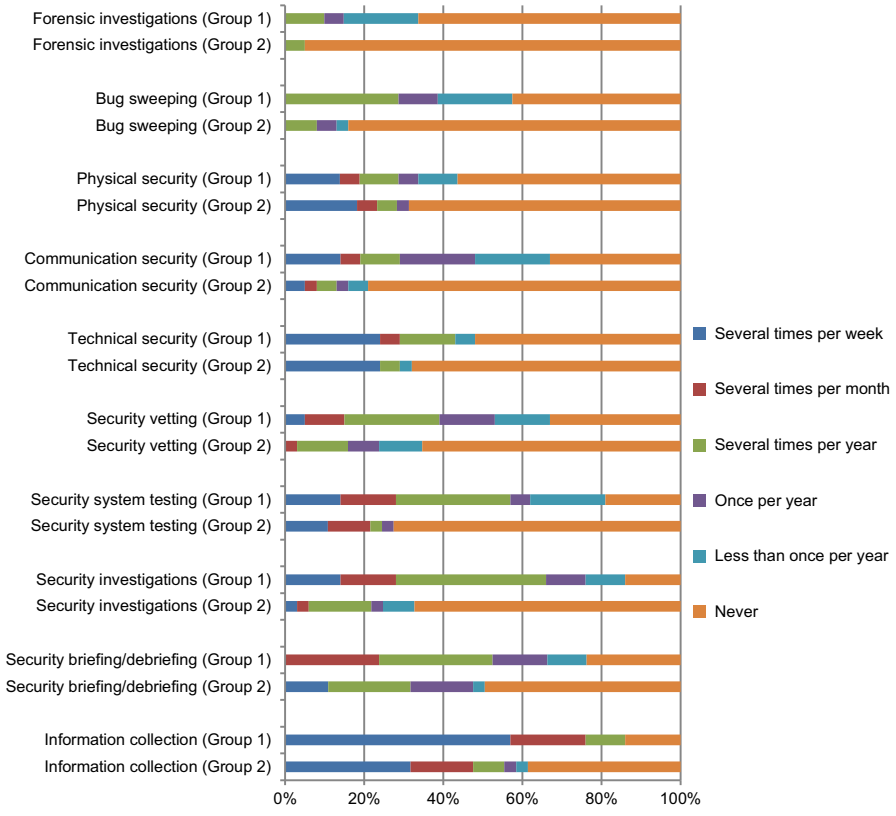

Chart 2 Frequency of conducting tasks for their clients: *Groups 1* and *2*

on average, conducted certain tasks that we identified as part of private intelligence or counterintelligence more often. Both groups conducted information collection most often (Group 1 = 86%, Group 2 = 61%), while forensic investigations were least often conducted (Group 1 = 33%, Group 2 = 5%).

Information collection in general was a key activity for all respondents. More specifically, respondents were focused on collecting information on clients' employees, which could be understood as part of counterintelligence. Regarding the question on how often they collect information for their clients on different topics, respondents in Group 1 again conducted the collection of information more often than respondents in Group 2 (Chart 3). The most common topic on which respondents were collecting information for their clients in both groups was the clients' employees (Group 1 = 81%, Group 2 = 37%), followed by information collection on their clients' business partners (Group 1 = 71%, Group 2 = 37%), their clients' competition (Group 1 = 67%, Group 2 = 34%), and the domestic market situation (Group 1 = 67%, Group 2 = 29%). The least frequent topic in both groups was information collection on the foreign market situation (Group 1 = 62%, Group 2 = 29%).

Regarding the question, how often respondents used listed methods to collect information, we found that respondents from Group 1 were again more likely to use the listed methods of information collection than respondents from Group 2 (Chart 4). Respondents from both groups listed communication recording (Group 1 = 14%, Group 2 = 5%), audio-recording (Group 1 = 52%, Group 2 = 18%), surveillance (Group 1 = 62%, Group 2 = 37%), and photography (Group 1 = 71%, Group 2 = 45%) as the least used methods of collecting information used. These methods were likely considered the most intrusive, and are often associated with the methods used by state security and intelligence services. The most commonly used information collection methods in Group 1 were open source media (86%), the internet (86%), official databases (86%), personal contacts (81%), observation (81%), online social media (76%), and networking (76%). For respondents in Group 2, the most frequently used methods to collect information were personal contacts (68%), official databases (66%), the internet (63%), online

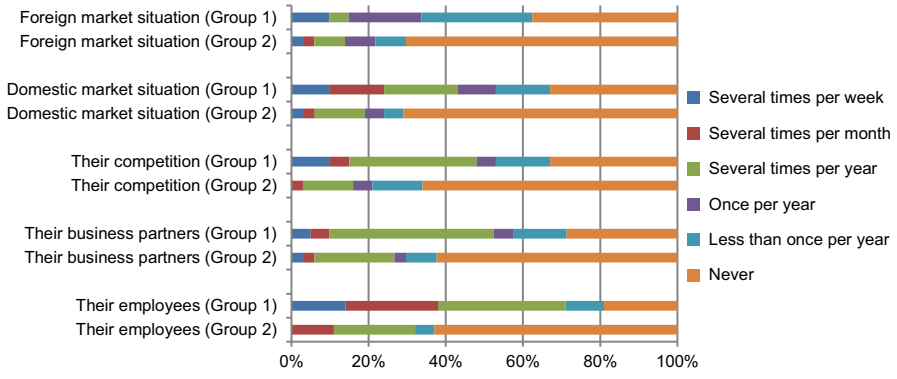

Chart 3 Areas of information collection: *Groups 1* and *2*

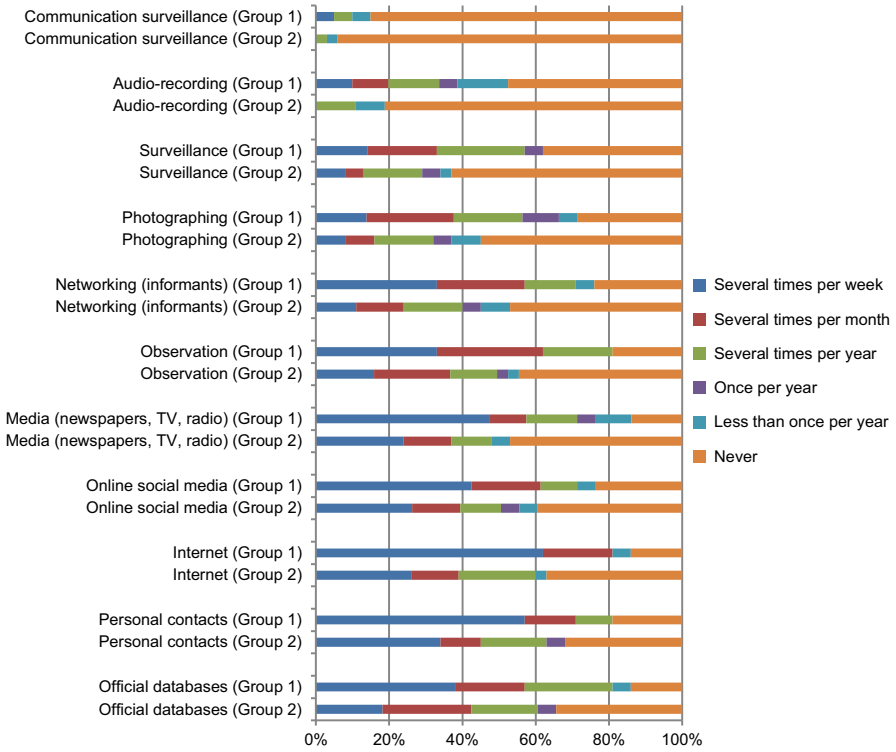

Chart 4 Information collection methods: *Groups 1* and *2*

social media (61%), observation (55%), open source media (53%), and networking (53%).

When asking respondents how often they witnessed different intelligence threats during their work (espionage, sabotage, subversion, terrorism, etc.), respondents from Group 1 again witnessed intelligence threats more often than respondents from Group 2 (Chart 5). The most common threat that respondents witnessed was espionage (Group 1 = 57%, Group 2 = 18%), followed by subversion (Group 1 = 33%, Group 2 = 13%), sabotage (Group 1 = 29%, Group 2 = 31%) and terrorism (Group 1 = 14%, Group 2 = 3%). Respondents from Group 2 on the other hand witnessed sabotage more often, following by subversion espionage and terrorism.

In the second, qualitative part, we asked all respondents a follow-up, open-ended question: who would they say is or could be conducting private intelligence or counterintelligence in Slovenia? Respondents' answers were limited and quite diverse. Three respondents said that they had never seen private intelligence in their line of work, or they never thought about it. Seven respondents tried to ignore the word private, and claimed that intelligence and counterintelligence can be conducted only by the state and that there is no such thing as private intelligence. Seven of the respondents also denounced the term private intelligence or counterintelligence, likely in order not to be associated with the state's intelligence

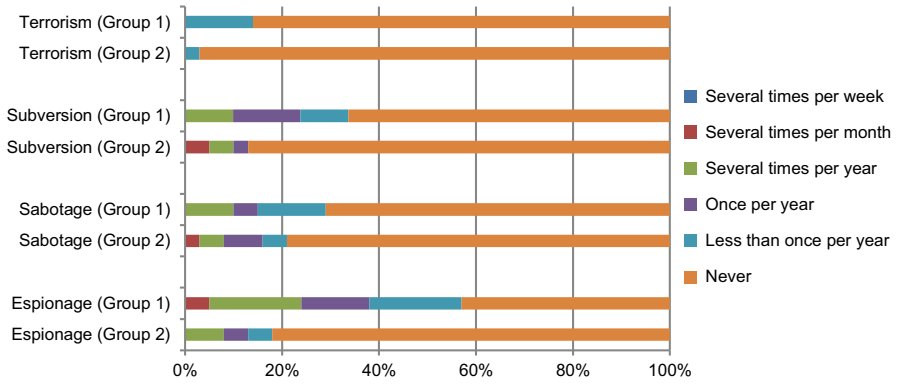

Chart 5 Intelligence threats: *Groups 1* and *2*

or counterintelligence activities. The last response could be explained by the notion that intelligence and counterintelligence have a bad reputation in post-socialist countries (Williams and Deletant 2001) to which Slovenia belongs. In previous socialist regimes, intelligence and security services had a fearsome reputation, and some of the respondents were likely trying to avoid being associated with that reputation. Nevertheless, 11 respondents identified private detectives and, to a lesser extent, private security companies as the main actors of private intelligence and counterintelligence. Additionally, eight respondents understood the term private intelligence or counterintelligence more broadly and mentioned private companies or their internal departments that deal with information collection.

Conclusion

Private intelligence in the West has evolved from its humble beginnings, mainly in private detective or security companies, and become a unique marketing service that is being utilized in a globalized world of multinational corporations, not limited with national borders. Clients of such services can often be countries and larger corporations that try to manage identified risks that could endanger their interests. Additionally, these clients also strive to protect their own knowledge and secrets and manage risks associated with leaks or theft of information. In accordance with the law, private intelligence can be a legitimate and normal economic activity. Private intelligence companies that provide intelligence and counterintelligence services do carry with them some risk for society at large. The state's intelligence services can intervene into one's privacy (a basic human right) in accordance with the law, but such interventions are strictly forbidden for private intelligence companies. Of course, this does not necessary mean that such activities do not exist. The importance of information in contemporary business and a technologically advanced and competitive, free-market environment puts severe pressure on private intelligence firms to acquire the best, most reliable information. This incentive for

profit can prevail in such environment and may increase one's willingness to misuse information and surveillance technology, and consequently break the law and endanger basic human rights, such as the right to privacy. Democratic countries have required several decades to establish effective control over their intelligence and security services, but private intelligence firms can be more elusive and more difficult to regulate in this matter as they are not under direct state control. One of the mechanisms of private companies to protect themselves from competitive intelligence is private counterintelligence, which includes strong protective measures.

The described developments in the field of private intelligence in Slovenia were analyzed through legal and practical aspects. The main legislation that enables private intelligence includes the Private Detective Activities Act (2011) and the Private Security Act (2011). Private Detective Activities Act (2011) allows private detectives to operate under certain legal conditions that enable them to gather data and information on behalf of their clients. Private Security Act (2011) allows private security personnel to also carry out passive counterintelligence measures, such as physical and technical security. There are however also strict legal limitations in regard to interfering with basic human rights, such as one's right of privacy.

In order to investigate practical dimensions of private intelligence in Slovenia, we conducted an online survey among private security industry entities (private detectives, private security companies, security consulting, and information security). We found out that based on their answers, respondents can be divided into two groups: a smaller Group 1, encompassing respondents who perceived their work as intelligence or counterintelligence, and a bigger Group 2, encompassing respondents who answered that they do not perceive their work as intelligence or counterintelligence. Group 1 was more often involved in activities that we considered to be private intelligence or counterintelligence. Although respondents from Group 2 said their work cannot be defined as private intelligence or counterintelligence, analysis of their answers shows that they were, albeit in smaller percentage, also involved in some activities, which we defined through theoretical aspects as being part of private intelligence or counterintelligence.

Because of the sensitivity of using the word 'intelligence,' it is not entirely possible to determine with certainty how widespread private intelligence is in Slovenia. Similarly, no private Slovenian company could be found that advertises its services explicitly as intelligence or counterintelligence. However, the theoretical model, legislation review and online survey revealed some elements of private intelligence in Slovenia, primarily in the work of private detectives and private security companies. Legislation and business practices have also shown that private counterintelligence is being practiced in Slovenia, though mostly in form of passive security measures.

As noted above, research on this topic is limited, and there are areas of research that could be done in the future to expand it. The paper was focused on a more defensive side of private intelligence activities in Slovenia, prioritizing protection of clients' information. And although, we could not find private companies in the Republics of Slovenia advertising their work as private intelligence, it was suggested in the qualitative part of the questionnaire by some respondents that they

believe private intelligence is being conducted by some corporate elements. Further research could illuminate this and would be welcomed. However, due to the secretive nature and also the negative connotation intelligence still has in Slovenia, such inquiries and research will likely prove to be quite challenging.

References

Barbulescu v. Romania [2016] ECHR 61496/08.

Bean, H. 2015. Privatizing intelligence. In *Routledge handbook of private security studies*, ed. R. Abrahamsen, and A. Leander, 79–88. New York: Routledge.

Blancke, S. 2011. *Private intelligence: Geheimdienstliche Aktivitäten nicht-staatlicher Akteure*. Wiesbaden: Springer.

Britovšek, J., and A. Sotlar. 2014. Zasebna obveščevalna dejavnost. *Varstvoslovje* 16 (3): 278–295.

Campbell, H.S. 2013a. Intelligence in the post Cold War period. Part I, the changed environment. *The Intelligencer* 19 (3): 45–52.

Campbell, H.S. 2013b. Intelligence in the post Cold War period. Part II, the impact of technology. *The Intelligencer* 20 (1): 57–65.

Central Intelligence Agency. 2017. Slovenia. In *The world factbook*. https://www.cia.gov/library/publications/the-world-factbook/geos/si.html.

Chesterman, S. 2008. 'We can't spy… if we can't buy!': The privatization of intelligence and the limits of outsourcing 'inherently governmental functions'. *European Journal of International Law* 19 (5): 1055–1074.

Code of Obligations. 2001, 2006, 2007. Official Gazette of the Republic of Slovenia (83/01, 28/06, 40/07).

Colby, E.W. 1976. Intelligence secrecy and security in a free society. *International Security* 1 (2): 3–14.

Companies Act (ZGD-1). 2006, 2008, 2009, 2011, 2012, 2013, 2015. Official Gazette of the Republic of Slovenia (42/06, 60/06, 10/08, 68/08, 42/09, 33/11, 91/11, 32/12, 57/12, 82/13, 55/15).

Constitution of the Republic of Slovenia. 1991, 1997, 2000, 2003, 2004, 2006, 2013. Official Gazette of the Republic of Slovenia (33/91-I, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13).

Copland v. The United Kingdom [2007] ECHR 62617/00.

Council of the EU. 2016. *Trade secrets protection*: *Council adopts new directive*. http://www.consilium.europa.eu/en/press/press-releases/2016/05/27-trade-secrets-new-directive/. Accessed 8 Sep 2016.

Criminal Code of the Republic of Slovenia. 2008, 2009, 2011, 2015, 2016. Official Gazette of the Republic of Slovenia (55/08, 66/08, 39/09, 91/11, 54/15, 38/16).

Dedijer, S. 2003. *Development and intelligence 2003–2053*. Working Paper, 2003/10. Lund: Research Policy Institute.

Dvoršak, H. 2003. Kako do finančnih podatkov. *Detektiv* 6 (1/2): 54.

Electronic Communications Act. 2012, 2013, 2015. Official Gazette of the Republic of Slovenia (109/12, 110/13, 81/15).

Employment Relationship Act. 2013. Official Gazette of the Republic of Slovenia (21/13, 78/13).

European Court of Human Rights. 1953/2010. *The European Convention on Human Rights*. Strasbourg: European Court of Human Rights.

General Assembly of the United Nations. 1948. *The Universal Declaration of Human Rights*. New York: General Assembly of the United Nations.

Gill, M., and J. Hart. 1999. Enforcing corporate security policy using private investigators. *European Journal on Criminal Policy and Research* 7 (2): 245–261.

Gill, P., and M. Phythian. 2006. *Intelligence in an insecure world*. Cambridge: Polity Press.

Gjerek, B. 2009. Taktika in metodika dela gospodarskih poizvedovalcev. Spec. Thesis, Faculty of Criminal Justice and Security, Ljubljana.

Guardiancich, I. 2016. Slovenia: The end of a success story? When a partial reform equilibrium turns bad. *Europe–Asia Studies* 68 (2): 205–231.

Halford v. The United Kingdom [1997] ECHR 20605/92.

Herman, M. 1996. *Intelligence power in peace and war*. Cambridge: University Press.

Hulnick, A.S. 2002. Risky business: Private sector intelligence in the United States. *Harvard International Review* 24 (3): 68–72.
Javers, E. 2011. Secrets and lies: The rise of corporate espionage in a global economy. *Georgetown Journal of International Affairs* 12 (1): 53–60.
1KA. 2016. *General description*. http://english.1ka.si/c/694/General_description/.
Keefe, R.P. 2010. Privatized spying: The emerging intelligence industry. In *The Oxford handbook of national security intelligence*, ed. K.L. Johnson, 296–309. Oxford: University Press.
Klemenčič, G. 2001. Varstvo elektronske zasebnosti. In *Internet in pravo*, ed. M. Potrč, 129–191. Ljubljana: Pasadena.
Lowenthal, M. 2009. *Intelligence, from secrets to policy*. Washington, DC: CQ Press.
Lowenthal, M. 2011. Intelligence analysis guide to its study. *The Intelligencer* 18 (3): 61–64.
Matey, D.G. 2005. Intelligence studies at the dawn of the 21st century: New possibilities and resources for a recent topic in international relations. *UNISCI Discussion Papers* 8 (May): 1–15.
Personal Data Protection Act (2004). 2004, 2007. Official Gazette of the Republic of Slovenia (86/04, 67/07).
Podbregar, I. 2005. *Preprečevanje poslovnega kriminala*. Kranj: Moderna organizacija.
Podbregar, I. 2006. Some patterns of industrial espionage. *Varstvoslovje* 8 (3/4): 323–331.
Private Detective Activities Act. 2011. Official Gazette of the Republic of Slovenia (17/11).
Private Security Act. 2011. Official Gazette of the Republic of Slovenia (17/11).
Prunckun, H. 2012. *Counterintelligence theory and practice*. Lanham: Rowman and Littlefield.
Shulsky, A., and G. Schmitt. 2002. *Silent warfare: Understanding the world of intelligence*. Washington, DC: Brassey's.
Sotlar, A., and J. Trivunović. 2012. Detektivi in varstvo zasebnosti v Republiki Sloveniji. *Varstvoslovje* 14 (3): 307–330.
van Steden, R., and R. Sarre. 2007. The growth of private security: Trends in the European Union. *Security Journal* 20 (4): 222–235.
Vrenko, I. 1999. Ekonomska in konkurenčna obveščevalna dejavnost – študija primera Slovenije. *Varstvoslovje* 1 (2): 31–44.
Vršec, M. 1993. *Varnost podjetja – tokrat drugače*. Ljubljana: Viharnik.
Warner, M. 2009. Intelligence as risk shifting. In *Intelligence theory: Key questions and debates*, ed. P. Gill, S. Marrin, and M. Phythian. London: Routledge.
Weiss, P.R. 2008. From cowboy-detectives to soldiers of fortune: The recrudescence of primitive accumulation security and its contradictions on the new frontiers of capitalist expansion. *Social Justice* 34 (3–4): 1–19.
Wheaton, K.J., and M.T. Beerbower. 2006. Towards a definition of intelligence. *Stanford Law and Policy Review* 17 (2): 319–331.
Whitehead, S. 2003. Corporate counterintelligence—Protecting business information. *Hi-tech Security Solutions Magazine*. http://www.securitysa.com/regular.aspx?pklregularid=1366.
Williams, K., and D. Deletant. 2001. *Security intelligence services in new democracies: The Czech Republic, Slovakia, and Romania*. London: Palgrave.
Wyss, M. 2011. *Zivile Nachrichtendienstsysteme im europäischen Umfeld der Schweiz*. Zürich: ETH.
Žaže, S. 2007. Meje dovoljenosti gospodarskega poizvedovanja. Spec. Thesis, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana.